

34. FINITE SIMPLE GROUPS

Classification of finite simple groups: There are 18 infinite families of simple groups and 26 “sporadic” groups. Of all of these groups you know:

- (1) The cyclic groups \mathbb{Z}_p are simple when p is prime.
- (2) The alternating groups A_n are simple if $n \geq 5$.

The other 16 infinite families come from finite fields. The easiest to describe are the *projective unimodular groups* $PSL(n, q)$. Today, I will tell you what these groups are and what are their basic properties.

34.1. Matrices over finite fields. We take $n \times n$ matrices with coefficients in the finite field $GF(q)$. They look like this:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad a, b, c, d \in GF(q)$$

Question: How many 2×2 matrices are there with coefficients in $GF(q)$?

Matrices are added and multiplied in the usual way, keeping in mind that the entries lie in the field $F = GF(q)$. For example, if $q = 3$ we get:

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}$$

The matrices on the left are called **elementary matrices** and they are denoted $E_{12}(2)$ and $E_{21}(2)$. The notation is: $E_{ij}(a)$ (with $i \neq j$) is the identity matrix with (i, j) entry changed to a . For example:

$$E_{31}(a) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & 0 & 1 \end{pmatrix}$$

Recall from linear algebra: Left multiplication by $E_{ij}(a)$ performs a row operation on a matrix and right multiplication by $E_{ij}(a)$ performs a column operation. In the above example, $XE_{21}(2)$ is the matrix X with twice the second column added to the first column.

Elementary matrices have determinant equal to 1. Therefore, any product of elementary matrices has determinant 1. For example:

$$\det \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix} = 2 - 4 = -2 = 1 \quad \in \mathbb{Z}_3 = GF(3)$$

Definition 34.1. If F is any field, let $GL(n, F)$ denote the group of all $n \times n$ invertible matrices with coefficients in the field F . This is the same as the set of all $n \times n$ matrices (with coefficients in F) whose

determinant is nonzero. Let $SL(n, F)$ denote the subgroup of $GL(n, F)$ consisting of matrices of determinant 1.

Theorem 34.2. $SL(n, F)$ is a normal subgroup of $GL(n, F)$.

Proof. $SL(n, F)$ is by definition the kernel of the homomorphism

$$\det : GL(n, F) \rightarrow F^\times$$

Therefore, $SL(n, F) \trianglelefteq GL(n, F)$. □

Notation $GL(n, q) := GL(n, GF(q))$ and $SL(n, q) := SL(n, GF(q))$.

34.2. orders of matrix groups. Question: What is the order of the group $GL(2, q)$?

Theorem 34.3.

$$|GL(2, q)| = (q^2 - 1)(q^2 - q)$$

Proof. There are a total of q^4 matrices (of size 2×2)

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

since there are q possibilities for each of the entries a, b, c, d . We need to know how many of these satisfy the equation:

$$ad - bc \neq 0$$

The first obvious point is that a, c cannot both be zero. So, there are $q^2 - 1$ possibilities for a, c .

Claim Once you choose a and c there are exactly $q^2 - q$ choices for b and d . (In other words, there are exactly q choices which don't work.)

The ones that won't work are the multiples of $\begin{pmatrix} a \\ c \end{pmatrix}$:

$$\det \begin{pmatrix} a & ax \\ c & cx \end{pmatrix} = acx - cax = 0$$

Any other choice of b, d will give an invertible matrix. This is because, if the second column is not a multiple of the first then then we can do an elementary operation to make one of the entries in the second column zero. For example:

$$AE_{12}(-a^{-1}b) = \begin{pmatrix} a & 0 \\ c & d - ca^{-1}b \end{pmatrix}$$

has determinant

$$a(d - ca^{-1}b) \neq 0$$

□

Corollary 34.4.

$$|SL(2, q)| = (q^2 - 1)q = q^3 - q$$

Proof. This follows from the isomorphism theorem which says that for any homomorphism $\phi : G \rightarrow H$, $G/\ker \phi \cong im\phi$. In this case the homomorphism is $\det : GL(n, q) \rightarrow F^\times$ with kernel $SL(n, q)$ which gives:

$$\frac{GL(n, q)}{SL(n, q)} \cong GF(q)^\times$$

So,

$$|SL(2, q)| = \frac{|GL(2, q)|}{|GF(q)^\times|} = \frac{(q^2 - 1)(q^2 - q)}{q - 1} = (q^2 - 1)q$$

□

34.3. centers of GL and SL . The center of $GL(n, F)$ is the group of all diagonal matrices with the same entry repeated along the diagonal. For example:

$$Z = Z(GL(3, F)) = \left\{ \begin{pmatrix} x & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x \end{pmatrix} : x \neq 0 \in F \right\}$$

If $F = GF(q)$ then, no matter what n is we get

$$|Z| = q - 1$$

Question: What is the intersection: $Z \cap SL(n, q)$?

We will discuss this next time.

Definition 34.5.

$$PSL(n, q) := \frac{SL(n, q)}{Z \cap SL(n, q)}$$

This is called the **projective unimodular group**

Theorem 34.6. $PSL(n, q)$ is simple except in the two cases $PSL(2, 2)$ and $PSL(2, 3)$.